Grid Information Service: Naming, Discovery and Cataloguing

Bill Johnston and Mike Helm

wejohnston@lbl.gov, M_Helm@lbl.gov

Issues

- Resource naming and discovery
- Grid Information Object naming and schema registration
- Grid people/entity naming (X.500 DNs)
- Grid entity certification (X.509 Certificate Authority) registration

Resource Naming and Discovery

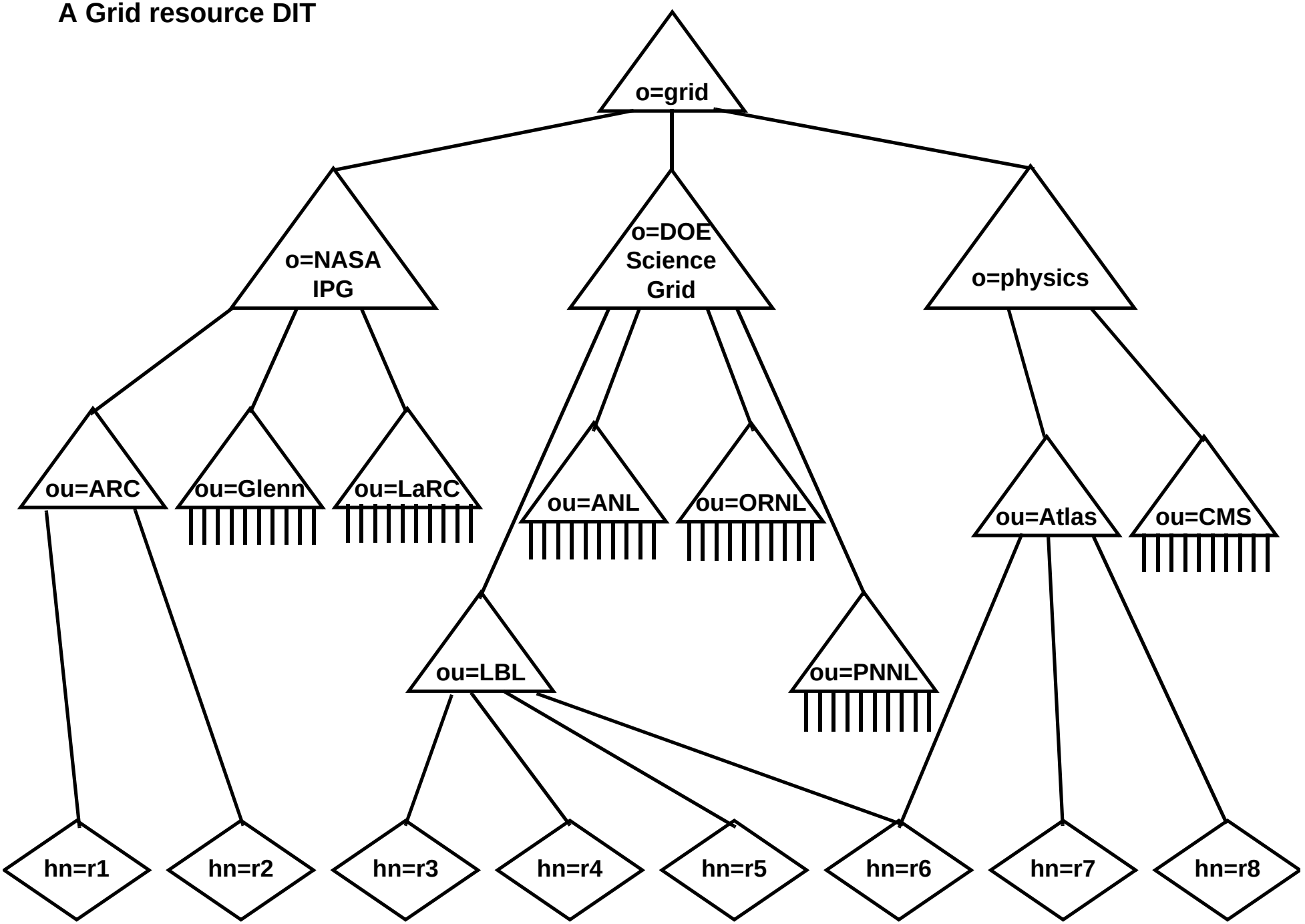
The service is currently provided by LDAP directory servers which provide persistent storage for named objects that have attributes. “Views” will provide a search scope appropriate to particular projects.

Specialized / project views resources can define “Grids” for virtual organizations of various sorts (e.g. Grids like NASA’s IPG and DOE’s Science Grid, and projects like the HEP’s Atlas, CMS, etc.).

- **Named objects in the Grid have characteristics specified by attributes and values**
- **The Grid Forum is defining schema for a standardized set of objects – e.g.**
  - **Grid::PhysicalResource**
  - **Grid::ImageResource**
  - **Grid::ComputeResource**
  - **Grid::OperatingSystemInformation**
  - **Grid::MemoryInformation**
  - **Grid::CacheInformation**
  - **Grid::BenchmarkInformation**
  - **Grid::CpuInformation**
  - **Grid::SystemDynamicInformation**

- **Resource discovery is done by a hierarchical search of the LDAP Directory Information Tree (“DIT”):**
- **LDAP permits the creation of nodes that represent the root of a project hierarchy – these nodes provide search scoping by establishing project “roots” that sit at the top of a hierarchy of project resources**

A Grid resource DIT



Example:

Within the Atlas Grid find all SPARC architecture machines:

- **start the search at o=grid, o=physics, ou=Atlas**
- **collect pointers to all LDAP objects that have the "architecture" attribute**
- **request and examine these objects for architecture==SPARC**

Need sufficient redundancy of directory servers so that local sites are not dependent on accessing remote servers to access local resources.

- **Both LDAP nodes and servers may be placed at appropriate tree and physical locations**

Grid Information Object Naming

Beyond Grid resources, there is a general need to ensure naming consistency for various catalogues:

- **Grid Information Object names and their schema**
- **Certification Authorities**
- **Database registries**

Strawman

A general naming consistency service can be provided using the infrastructure of a Grid resource naming service. This service would provide a namespace root that is, or comes close to, a “global” registry for top-level names.

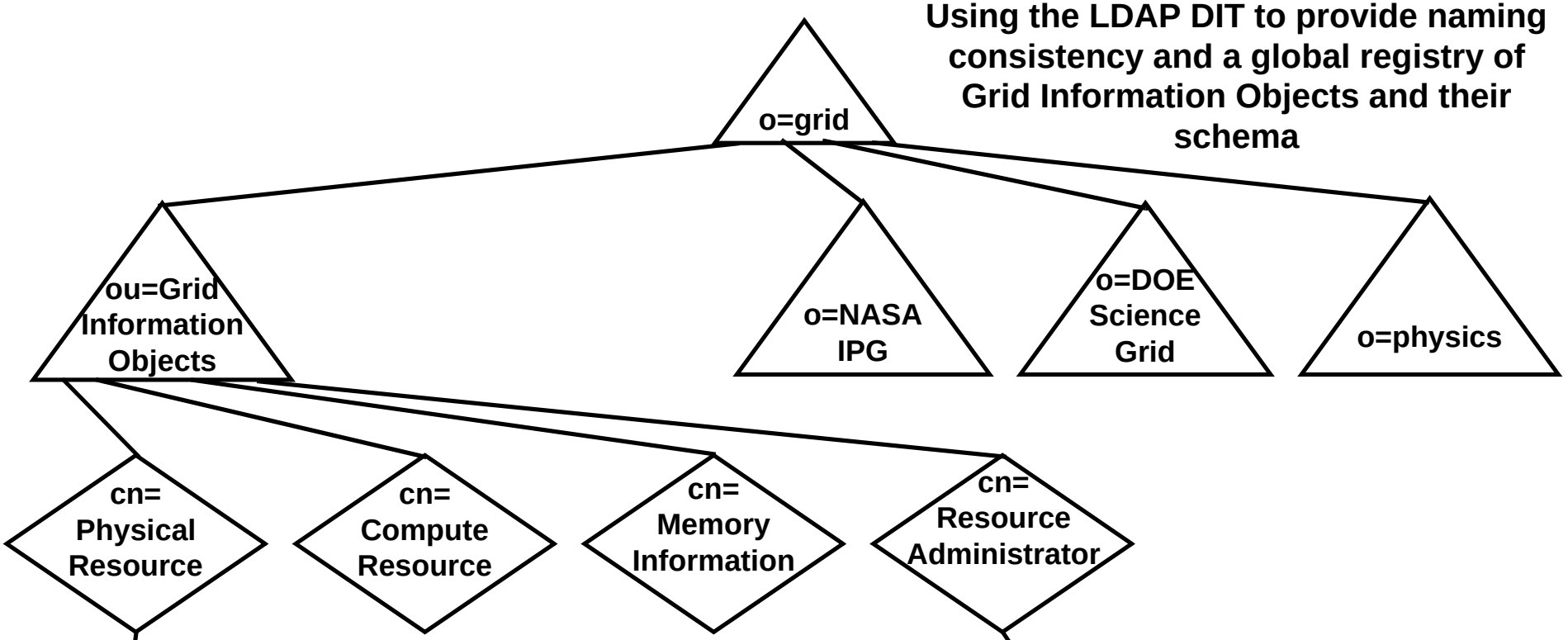
That is, *the LDAP server that provides the top of the Grid DIT (o=Grid) can also be used as the top of a set of catalogues that index various objects of interest in the Grid community, and provide naming consistency and discovery for those objects.*

Schema catalogue example:

To provide globally unique names for Grid Information Objects (“GIO”) create an ou=GridInformationObjects DIT node that indexes GIO names as DIT nodes (e.g. cn=ComputeResource)

To use this as a GIO schema catalogue, provide the GIO definitions as an attribute of the leaf nodes of this branch of the DIT.

Using the LDAP DIT to provide naming consistency and a global registry of Grid Information Objects and their schema



the value of the attribute "schema"

```
Grid::PhysicalResource OBJECT-CLASS ::= {
  SUBCLASS OF { Grid::Top }
  RDN = rn (resourceName)
  AGGREGATES{
     Grid::Locality
  }
  MAY CONTAIN{
    resourceOwner              :: dn,
    resourceAdministrator      :: dn,
    resourceProvider           :: dn,
    description                :: cis,
    documentation              :: cis,
    imageObject                :: dn,
    url                        :: url,
  }
}
```

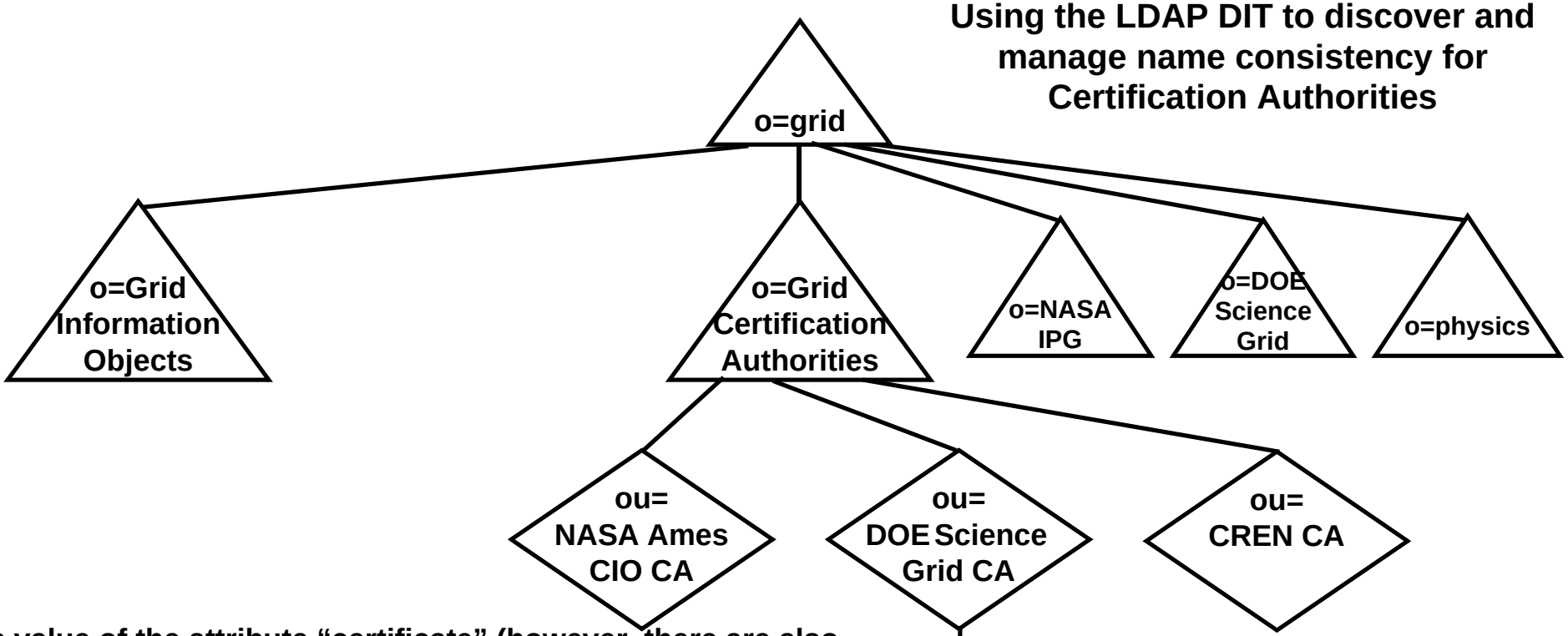
```
Grid::ResourceAdministrator OBJECT CLASS
  SUBCLASS OF Grid::Person
  RDN = cn (commonName)
  MAY CONTAIN {
    administratedResource          :: cis,
    responsibility   :: cis
    seeAlso :: dn
  }
```

CA registration example:

To provide a list of CAs that certify Grid users, and to provide the public keys of these CAs, create an o=GridCertificationAuthorities node that indexes X.509 CAs and provides their location and public keys as attributes of that DIT leaf

This is a catalogue of CAs, not a hierarchy of CAs. These CAs do not necessarily have any relationship to each other (e.g. trust) except that they all provide certificates to Grid users.

Using the LDAP DIT to discover and manage name consistency for Certification Authorities



the value of the attribute "certificate" (however, there are also standard attributes for all of the components of an X.509 cert.)

```
Certificate:
    Data:
        Version: v3 (0x2)
        Serial Number: 109 (0x6d)
        Signature Algorithm: PKCS #1 MD5 With RSA Encryption
        Issuer: CN=IDCG-CA, OU=ICSD, O=Lawrence Berkeley National Laboratory, C=US
        Validity:
            Not Before: Tue Jul 27 18:38:44 1999
            Not  After: Thu Jul 26 18:38:44 2001
        Subject: CN=IDCG-CA, OU=ICSD, O=Lawrence Berkeley National Laboratory, C=US
        Subject Public Key Info:
            Algorithm: PKCS #1 RSA Encryption
            Public Key:
                Modulus:
    00:c0:ae:5c:be:b6:75:f9:79:6e:ef:e0:a4:f9:09:57:ff:23:04:7c:ac:39:2a:9e:20:d4:ab:7e:31:ff:0a:ab:29:b3:34:01:8f:92:57:68:44:1f:3f:8c:08:38:12:96:63:ce:
                5d:fc:04:a6:55:d6:e4:86:18:5e:a2:77:f9:d2:b4:e9:eb:7b:99:4a:1d:3a:10:01:fb:46:fa:6b:c7:55:c2:e9:75:fa:04:70:12:2f:34:bd:fb:78:f9:6b:
                c3:51:41:cc:65:08:aa:dd:4a:85:4e:c3:cd:fb: 4f:6c:5b:ed:a9:6a:a5:cd:41:9b:c1:ab:6a:fe:eb:fa:2f:33: 83:aa:57
```

Grid Information Service: A Suite of Grid Catalogues

Where this is headed is to use a single approach and infrastructure to name and discover many different objects of interest in the Grid.

A Grid Information Service: Resources, Object Schema Catalogues, CA Registry